E-FILED
IN COUNTY CLERK'S OFFICE
PIERCE COUNTY, WASHINGTON

August 29 2023 3:27 PM

CONSTANCE R. WHITE
COUNTY CLERK
NO: 23-2-09361-1

IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR PIERCE COUNTY

BASSAM ZAAFAN, individually and on behalf of all others similarly situated, Plaintiff, v. UMPQUA BANK, Defendant.	CASE NO. **CLASS ACTION COMPLAINT FOR:** **(1) NEGLIGENCE;** **(2) BREACH OF THIRD PARTY BENEFICIARY CONTRACT;** **(3) VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, RCW 19.86**

Plaintiff Bassam Zaafan, by and through his counsel, brings this Class Action Complaint against Defendant Umpqua Bank ("Umpqua"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that Plaintiff and Class Members, as customers of Umpqua, entrusted to it, including, without limitation, their names and Social Security numbers (collectively, "personally identifiable information" or "PII").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. Defendant is a community bank based in Oregon that recently merged with Columbia Bank in Washington.

3. Plaintiff and Class Members are current and former customers of Umpqua.

4. As a condition of receiving its services, Umpqua requires that its customers, including Plaintiff and Class Members, entrust it with highly sensitive personally identifiable information ("PII"), including but not limited to their names and Social Security numbers.

5. Plaintiff and Class Members provided their PII to Umpqua with the reasonable expectation and on the mutual understanding that Umpqua would comply with its obligations to keep that information confidential and secure from unauthorized access.

6. Umpqua derives a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without it, Umpqua could not perform its services.

7. Umpqua had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its vendors and affiliates for their own cybersecurity. Umpqua has a legal duty to keep consumers' PII safe and confidential.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Umpqua assumed legal and equitable duties to ensure the protection of that PII, and it knew or should have known that it was thus responsible for protecting Plaintiff's and Class Members' PII from disclosure.

9. On or about August 11, 2023, Umpqua began sending Plaintiff and other Class Members notice (the "Notice Letter") informing them that their PII had been exposed as a result of a breach of a tool used by one of Umpqua's vendors to store and transfer PII (the "Data Breach").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

10. Noticeably absent from the Notice Letter are details of the root cause of the Data Breach, the vulnerabilities that were exploited, and the remedial measures that Umpqua undertook to ensure such a breach does not happen again. To date, these critical facts have not been explained or clarified to Plaintiff or the Class Members, who have a vested interest in ensuring that their PII remains protected.

11. In fact, the attacker accessed and acquired files that Umpqua shared with its vendor containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware and software containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to, among other things, negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; and (v) the continued and certainly increased risk to their PII a, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Bassam Zaafan is, and at all times relevant, has been a citizen of Tacoma, Washington. Plaintiff Zaafan has no intention of moving to a different state in the immediate future. Plaintiff Zaafan received an email from Defendant on or around June 22, 2023, regarding the Data Breach and a Notice of Data Breach letter from Defendant.

16. Defendant Umpqua Bank is an Oregon state-chartered bank with its principal place of business at 5005 Meadows Road, Suite 400, Lake Oswego, Oregon.

III. JURISDICTION AND VENUE

17. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010 and RCW 4.92.090.

18. This Court has personal jurisdiction over Defendant because it regularly conducts business in Washington, including in this County, and because its conduct with

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

respect to Plaintiff, including its collection of Plaintiff's PII and the duties it assumed with respect to Plaintiff, occurred in this County. Defendant recently merged with Columbia Bank, which is headquartered in this County.

19. Venue is proper in this Court pursuant to RCW 4.92.010(1) and RCW 4.12.020(3) because Plaintiff resides in Pierce County where the cause of action arose.

IV. FACTUAL BACKGROUND

A. The Data Breach

20. As outlined above, Umpqua admitted that its vendor was the subject of a massive data breach that affected millions of its customers. Between May 27 to May 30, 2023, unauthorized third-party cybercriminals exploited a vulnerability in the file transfer protocol software Umpqua's vendor used to store and transfer Umpqua's customers' data.[1]

21. The customer PII the hackers accessed include names and Social Security numbers.[2]

22. Umpqua had obligations to Plaintiff and to Class Members to safeguard their PII and to protect that PII from unauthorized access and disclosure, including by ensuring that its vendors would protect that PII. Indeed, Plaintiff and Class Members provided their PII to Umpqua with the reasonable expectation and mutual understanding that Umpqua, and anyone Umpqua contracted with, would comply with its obligations to keep such information confidential and secure from unauthorized access. Umpqua's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies before the Data Breach.

---

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7589df9f-75b6-417f-afa0-68eeec2e7de9.shtml (last visited on August 29, 2023).

[2] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

23. Umpqua also promises to keep the PII it collects secure, even when it provides that PII to third parties. In its Privacy Policy, Umpqua promises that it "use[s] reasonable physical, electronic, and procedural safeguards that comply with federal standards to protect and limit access to personal information. This includes device safeguards and secured files and buildings."[3]

24. It also promises that "We protect your personal information commensurate with its degree of sensitivity."[4]

25. As a result of the Data Breach, Umpqua is urging affected consumers to monitor their accounts for suspicious activity and to safeguard themselves against possible fraud.[5] Furthermore, numerous data security experts are also suggesting that affected consumers take steps to protect their identities.

B. Plaintiff Expected Umpqua and its Vendors to Keep His Information Secure.

Plaintiff Bassam Zaafan's Experience

26. Plaintiff Bassam Zaafan is a customer of Umpqua Bank.

27. Plaintiff Zaafan provided his PII when he opened his account with Defendant in or around May of 2023.

28. Plaintiff Zaafan is very careful about sharing his sensitive Private Information. Plaintiff Zaafan has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

29. Plaintiff Zaafan first learned of the Data Breach after receiving an email from Defendant on or around June 22, 2023, and then a Notice of Data Breach letter notifying him that Defendant suffered a data breach roughly one month prior and that his PII had been

[3] *See* Privacy at Columbia Banking Systems, Inc., *available at* https://www.umpquabank.com/privacy/ (last visited on August 29, 2023).
[4] *Id.*
[5] *See Supra*, at Note No. 1.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

30. The Notice of Data Breach letter indicated that the PII involved in the Data Breach may have included Plaintiff Zaafan's full name, and Social Security number.

31. As a result of the Data Breach, Plaintiff Zaafan made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice of Data Breach letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

32. As a result of the Data Breach, Plaintiff Zaafan has suffered fraudulent activity immediately following the Data Breach. Specifically, an unauthorized third party attempted to open up a new credit card under his name, and an unauthorized third party withdrew $300.00 out of his bank account on or around August 16, 2023. Since the Data Breach, Plaintiff Zaafan has also suffered from multiple scam text messages which are designed to trick Plaintiff Zaafan into disclosing his PII.

33. Plaintiff Zaafan has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Zaafan has already spent more than 10 hours trying to fix issues stemming from the Data Breach.

34. Plaintiff Zaafan suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Zaafan; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud. In fact, because his Social Security number is impacted, Plaintiff Zaafan faces this risk for his lifetime.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

35. As a result of the Data Breach, Plaintiff Zaafan has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Zaafan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Indeed, Plaintiff Zaafan has already suffered fraud as a result of the Data Breach.

36. As a result of the Data Breach, Plaintiff Zaafan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Zaafan will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

C. FTC Security Guidelines Concerning PII

37. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

38. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

39. In 2016, the FTC provided updated security guidelines in a publication titled Protecting Personal Information: A Guide for Business. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

programs; and pay particular attention to the security of web applications—the software used to inform visitors to a company's website and to retrieve information from the visitors.

40. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the industry; and verify that third parties with access to sensitive information use reasonable security measures.

41. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

42. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> "When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security."[6]

43. Umpqua was aware or should have been aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Umpqua violated its obligations under Section 5 of the FTC Act.

D. Umpqua Was on Notice of Data Threats and the Inadequacy of Its Vendor's Data Security.

44. Umpqua was on notice that companies maintaining large amounts of PII during their regular course of business are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this case.

45. At all relevant times, Umpqua knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, Umpqua failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyber-attacks that Umpqua should have anticipated and guarded against.

46. It is well known among companies that store PII that sensitive information—such as the Social Security numbers accessed in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, Business Insider noted that "[d]ata breaches are on the

[6] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[7]

47. In light of recent high-profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Umpqua knew or should have known that its electronic records would be targeted by cybercriminals.

48. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

E. The Data Breach Harmed Plaintiff and Class Members

49. Plaintiff and Class Members have suffered and will continue to suffer harm because of the Data Breach.

50. Plaintiff and Class Members face a present, imminent, and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach for their respective lifetimes. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI—thereby risking prosecution by listing it for sale on the dark web—if the PII and PHI was not valuable to malicious actors.

[7] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

51. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

52. Malicious actors use PII and PHI to gain access to Class Members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

53. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

54. Umpqua issued misleading public statements about the Data Breach, including its data breach notification letters, in which it attempts to downplay the seriousness of the Data Breach by stating that there is "no evidence at this time that your personal information has been used in an unauthorized way."[8]

55. Umpqua has also vaguely stated that it "immediately worked with our vendor to ensure that they had resolved the vulnerability to keep our customer information safe following the incident and moving forward" without giving any details of what steps, exactly, it took. Plaintiff and Class Members are thus left to guess whether Umpqua has, in fact, addressed

[8] *See Supra*, at Note No. 1.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the root causes of the Data Breach to ensure that Plaintiff and Class Members' PII cannot be accessed again.[9]

56. Umpqua's intentionally misleading public statements ignore the serious harm its security flaws caused to the Class. Even worse, those statements could convince Class Members that they do not need to take steps to protect themselves.

57. The data security community agrees that the PII compromised in the Data Breach greatly increases Class Members' risk of identity theft and fraud.

58. As Justin Fier, senior vice president for AI security company Darktrace, observed following a recent data breach at T-Mobile, "[t]here are dozens of ways that the information that was stolen could be weaponized." He added that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates.[10]

59. Criminals can use the PII that Umpqua lost to target Class Members for imposter scams, a type of fraud initiated by a person who pretends to be someone the victim can trust in order to steal sensitive data or money.[11]

60. The PII accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again.

61. Malicious actors can also use Class Members' PII to open new financial accounts, open new utility accounts, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

---

[9] *Id.*

[10] https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/ (last visited on August 29, 2023).

[11] *See* https://consumer.ftc.gov/features/imposter-scams (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

62. As established above, the PII accessed in the Data Breach is also very valuable to Umpqua. Umpqua collects, retains, and uses this information to increase its profits. Umpqua's customers value the privacy of this information and expect Umpqua to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Umpqua, provided their PII to Umpqua, and/or paid the same prices for Umpqua's goods and services had they known Umpqua did not implement reasonable security measures to protect PII. Umpqua states that it "develop[s] trust and build[s] mutually beneficial relationships by respecting your privacy and your choices."[12] Customers expect that the payments they make to Umpqua incorporate the costs to implement reasonable security measures to protect customers' PII as part of protecting their PII and respecting their privacy.

63. Indeed, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

64. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly

[12] *See Supra*, at Note No. 3.

[13] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en (last visited on August 29, 2023).

[14] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, and it can become more valuable to thieves and more damaging to victims.

65. The PII accessed in the Data Breach is also very valuable to Plaintiff and Class Members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to Wi-Fi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class Members' PII has been compromised and lost significant value.

66. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

67. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

68. Due to the immutable nature of the personal information impacted here, Plaintiff and Class Members will face a risk of injury due to the Data Breach for their

[15] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1 (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

respective lifetimes. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collection agencies. Plaintiff and Class Members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

69. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

70. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

71. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[16]

[16] *See* https://www.gao.gov/assets/gao-07-737.pdf (last visited on August 29, 2023).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

72. Plaintiff and Class Members have failed to receive the value of the Umpqua services for which their insurance companies paid.

F. Defendant Failed to Take Reasonable Steps to Protect its Customers' PII

73. Umpqua requires its customers to provide a significant amount of highly personal and confidential PII to purchase its services. Umpqua collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

74. Umpqua has legal duties to protect its customers' PII by implementing reasonable security features. This duty is further defined by federal and state guidelines and laws, including the FTC Act, as well as industry norms.

75. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiff's and Class Members' PII was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiff and Class Members were harmed.

76. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members and ensuring that its vendor did so as well.

77. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

78. Experts have identified several best practices that businesses like Umpqua should implement at a minimum, including, but not limited to: educating all employees; requiring strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

79. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

80. When using a file transfer protocol, moreover, best cybersecurity practices include not storing data or information longer than necessary to accomplish the transfer. By storing Plaintiff's and Class Members' PII in its file transfer protocol longer than was necessary to accomplish the transfer, Umpqua's vendor—for whom Umpqua was responsible—left Plaintiff's and Class Members' PII vulnerable to access and theft, which is what ultimately happened.

81. The Data Breach was a reasonably foreseeable consequence of Defendant's failure to ensure that its vendors used adequate security systems. Umpqua certainly has the resources to ensure that its vendors implement reasonable security systems to prevent or limit damage from data breaches. Even so, Umpqua failed to properly invest in that data security. Had Umpqua ensured that its vendors implemented reasonable data security systems and procedures (i.e., followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from accessing its customers' PII.

82. Umpqua's failure to ensure that its vendors implemented reasonable security systems has caused Plaintiff and Class Members to suffer and continue to suffer harm that adversely impact Plaintiff and Class Members economically, emotionally, and/or socially. As

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

discussed above, Plaintiff and Class Members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently sift out phishing communications to limit potential adverse effects of the Data Breach, regardless of whether any Class Member ultimately falls victim to identity theft.

83. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) diminution in value of their PII; (iv) the certain, ongoing, and imminent threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (v) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; and/or (vi) nominal damages.

84. Even though Umpqua has decided to offer free credit monitoring for two years to affected individuals, this is insufficient to protect Plaintiff and Class Members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiff and the Classes significant time and effort.

85. Plaintiff and Class Members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

86. Concurrently with the filing of this Complaint, Plaintiff is providing Umpqua with written notice of its breach of its Privacy Policy, which constitutes part of its contract with Plaintiff and Umpqua's customers. If Umpqua does not timely rectify its data security practices

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

in line with Plaintiff's notice, Plaintiff will amend this Complaint to include an action for Breach of Contract against Defendant.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Civil Rule 23 as representative of the Class defined as follows:

The Washington Class: All Washington residents whose data was accessed in the Data Breach.

88. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

89. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact Class Members.

90. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class numbers in the hundreds of thousands.

91. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all Class Members had their PII accessed in the Data Breach and were harmed as a result.

92. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to those of the classes and is aligned with Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Members' interests because Plaintiff was subject to the same Data Breach as Class Members and faces similar threats due to the Data Breach as Class Members. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes.

93. Commonality and Predominance: There are questions of law and fact common to the Class. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiff and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their personal information, and to ensure that its vendors did so as well;

b. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' PII;

c. Whether Defendant breached its duty to implement reasonable security systems to protect Plaintiff's and Class Members' PII, and to ensure that its vendors did so as well;

d. Whether Defendant breached its contractual obligations to its customers to protect Plaintiff's and Class Members' PII;

e. Whether Plaintiff and Class Members were intended third-party beneficiaries of Defendant's contract with its vendor;

f. Whether Defendant's breach of its duty to implement reasonable security systems, and its duty to ensure that its vendors did the same, directly and/or proximately caused damages to Plaintiff and Class Members;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

g. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

h. When Defendant learned of the Data Breach and whether its response was adequate;

i. Whether Plaintiff and other Class Members are entitled to credit monitoring and other injunctive relief; and,

j. Whether Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

94. Defendant has engaged in a common course of conduct, and Class Members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII and to ensure that the vendors to whom it provided Plaintiff's and Class Members' PII did the same.

95. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

96. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

97. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

98. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by failing to ensure that the third parties to whom it provided Plaintiff's and Class Members' PII implemented reasonable security procedures and practices to protect that PII. Among other things, Defendant failed to ensure that third party vendors: (i) implemented security systems and practices consistent with federal and state laws and guidelines; and (ii) implemented security systems and practices consistent with industry norms.

99. Defendant knew or should have known that Plaintiff's and Class Members' PII was highly sought after by cyber criminals and that Plaintiff and Class Members would suffer significant harm if their PII was compromised by hackers.

100. Defendant also knew or should have known that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiff and Class Members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs.

101. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members entrusted Defendant with several pieces of Plaintiff's and Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Members' PII so that Defendant would provide services to them. Defendant's customers were required to provide this PII when purchasing or attempting to purchase Defendant's services. Plaintiff and Class Members were led to believe Defendant would take reasonable precautions to protect their PII and would timely inform them if their PII was compromised, which Defendant failed to do.

102. The harm that Plaintiff and Class Members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to ensure that the third parties to whom it provided PII enacted reasonable security procedures and practices, and Plaintiff and Class Members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes.

103. But-for Defendant's breach of its duty of care, the Data Breach would not have occurred and Plaintiff's and Class Members' PII would not have been accessed by an unauthorized and malicious party.

104. As a direct and proximate result of the Defendant's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, among other things, (1) a present and imminent, immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their Private Information, for which there is a well-established

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference the foregoing allegations of fact as if fully set forth herein.

106. Defendant entered into a written contract with its vendor to provide certain services for which Defendant's vendor required Plaintiff's and Class Members' PII.

107. In exchange, on information and belief, Defendant and its vendor agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

108. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its vendor.

109. Defendant and/or its vendor breached the contract it entered into by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, (iii) failing to perform due diligence and to verify, audit, or monitor the integrity of third party networks on which it shared PII, and (iv) failing to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

110. Plaintiff and Class Members were harmed by Defendant's breach of its contract with its vendor, its vendor's breach of its contract with Defendant, or both, as such

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

COUNT III
Violation of the Washington Consumer Protection Act, RCW 19.86
(On Behalf of Plaintiff and the Class)

111. Plaintiff incorporates by reference the foregoing allegations of fact as if fully set forth herein.

112. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

113. Defendant is a "person" as described in RWC 19.86.010(1).

114. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

115. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

116. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, among other things, knowingly failing to ensure the safeguarding and protection of Plaintiff's and Class Members' PII by the entities to whom it provided that PII, and by violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

117. Defendant also violated the CPA by concealing from Plaintiff and Class Members information regarding the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII and identities.

118. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

119. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

120. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, among other things, (1) a present and imminent, immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

confidentiality of their PII; (5) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

121. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to ensure the safeguarding and protection of Plaintiff's and Class Members' PII by the entities to whom it provides that PII.

122. Plaintiff, on behalf of himself and Class Members, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff, on behalf of himself and Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000.00 per Class Member.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff makes the following prayer for relief, individually and on behalf of the proposed Class:

A. An order certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiff and his counsel to represent the Class;

B. An order awarding Plaintiff and Class members monetary relief, including actual damages;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

C. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein and compelling Defendant to utilize appropriate methods and policies with respect to maintaining the security of its systems;

D. An award of costs of suit and attorneys' fees, as allowable by law;

E. An award of pre-judgment and post-judgment interest, as provided by law;

F. Leave to amend this Complaint to conform to the evidence produced at trial; and

G. Such other and further relief as this Court may deem just and proper.

Dated: August 29, 2023

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: s/ *Kaleigh N. Boyd*

Kaleigh N. Boyd, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992
kboyd@tousley.com

M. Anderson Berry*
aberry@justice4you.com
Gregory Haroutunian*
gharoutunian@justice4you.com
Brandon P. Jack*
bjack@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

*Pro Hac Vice Application Forthcoming

Attorneys for Plaintiff and the Class